PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 9

Case No. DP-2206-B9897

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012

And

Tokyo Century Leasing (Singapore) Pte. Ltd.

… *Organisation*

DECISION

Tokyo Century Leasing (Singapore) Pte. Ltd.

Lew Chuen Hong, Commissioner - Case No. DP-2206-B9897

4 September 2023

Introduction

1 On 14 June 2022, the Personal Data Protection Commission (the **"Commission**") was notified by Tokyo Century Leasing (Singapore) Pte. Ltd. (the "**Organisation**") of a ransomware attack which resulted in the encryption of the personal data of 141,412 individuals ("**Incident**").

2 The Organisation requested that the investigation be handled under the Commission's Expedited Breach Decision Procedure. The Organisation voluntarily provided and admitted to the facts set out below, and admitted that it had failed to implement reasonable security arrangements to protect the personal data accessed and encrypted during the Incident, in breach of section 24 of the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

3 The Organisation is in the leasing and hire-purchase business. It operates a website through which existing or potential customers may submit applications to enter into hire-purchase or leasing agreements.

4 On 12 June 2022, the Organisation was notified by a customer that he was unable to submit an online application. The Organisation conducted an internal investigation and discovered that 7 servers and 6 employee computers had been infected with ransomware, resulting in the encryption of the personal data of 141,412 individuals, comprising:

a) 111,156 customers whose personal data consisted of name, NRIC number, date of birth, address, contact number, income statement, email address, employer information, bank account, and additionally for foreign customers, their passport numbers and employment pass numbers;

b) 30,220 guarantors whose personal data consisted of name, NRIC number, date of birth, address, contact number, income statement, email address, employer information, and bank account; and

c) 36 employees whose personal data consisted of name, NRIC number, date of birth, address, contact number, email address, bank account, resume information, and medical check-up information.

(collectively the "**Subject Data**")

5 The Subject Data was encrypted by a virus with the extension ".myghost". The Organisation also discovered a ransom note instructing the Organisation to contact "apichai[@]keemail.me" or "teeraanu[@]tuta.io" to obtain the decryption key, failing

which the Subject Data would be leaked. The ransom note did not specify a ransom amount. The Organisation did not respond to the ransom note.

6 The Organisation notified the Commission of the Incident on 14 June 2022. On 8 July 2022, the Organisation requested that the investigation be handled under the Commission's Expedited Breach Decision Procedure, and in a statement by its Managing Director dated 29 July 2022, admitted to a breach of section 24 of the PDPA.

7 Investigations were conducted between 14 June 2022 and October 2022, comprising the efforts of an IT forensic investigation firm engaged by the Organisation's parent organisation, and the Commission's own investigations. The investigations revealed that:

a) A malicious encryption programme "Stager.exe" had been executed on at least 3 servers by a compromised administrator account through Remote Desktop Connections;[1]

b) The IP address of each of the Remote Desktop Connections was generated by a FortiGate 100E Virtual Private Network ("**VPN**") and firewall device ("**Device**") in use by the Organisation since September 2019;

c) The software installed on the Device was the outdated version 6.0.4 of FortiOS and had a known vulnerability CVE-2018-13379 ("**Vulnerability**").[2]

[1] A Remote Desktop Connection refers to the connection and control by a user to a target device (such as a computer) remotely through the internet or other network.
[2] This is the same vulnerability that may have been exploited in the data breach incident which is the subject of the Commission's decision in *The Law Society of Singapore* [2023] SGPDPC 4.

The effect of the Vulnerability was that a malicious actor could, via the internet, remotely access system files on the Device, specifically "sslvpn_websession", containing the username and password of a VPN session. With such details, the malicious actor would be able to gain access to the VPN to which the target's (in this case, the Organisation) devices were connected;

d) The most likely cause of the Incident was that malicious actor(s) exploited the Vulnerability, thereby gaining access to the Organisation's VPN. The malicious actor(s) in turn compromised one of the Organisation's administrator accounts, gaining access to the Subject Data stored on the Organisations servers and computers. However, no evidence was discovered to indicate that the Subject Data had been exfiltrated;

e) The Device's manufacturer released a patch in May 2019 to address the Vulnerability,[3] but the patch had not been installed by the time of the Incident. The Organisation informed the Commission that while its IT vendor had the responsibility of upgrading the Organisation's firewall, such upgrading / patching was only triggered upon request by the Organisation. However, the Organisation was unaware of the patch, did not have processes in place to manage software patches, and therefore did not request its IT vendor to patch the Vulnerability; and

[3] Fortinet, Inc, "FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests" (FortiGuard Labs, 24 May 2019) <https://www.fortiguard.com/psirt/FG-IR-18-384> accessed 23 March 2023.

f) The Organisation had not implemented Multi-Factor Authentication ("**MFA**") for its administrator accounts at the time of the Incident.

Remedial Action

8 After the Incident, the Organisation took the following remedial actions:

a) Reported the Incident to the Singapore Police Force and the Commission, within 72 hours of the discovery by the Organisation of the same;

b) Published a notice of the Incident on its website, and engaged an external call centre to provide hotline services to affected customers;

c) Conducted anti-virus scans on all its computers;

d) Engaged an IT forensic investigation firm to scan and monitor the internet for the Subject Data. The IT forensic investigation firm did not detect any disclosure of the same on the internet;

e) Patched the Vulnerability and its Windows systems;

f) Changed the passwords for its administrator accounts for all its servers and critical network equipment; and

g) Implemented MFA for access to its VPN.

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation

9 Under section 24 of the PDPA an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks (the "**Protection Obligation**").

10 The reasonableness of an organisation's security arrangements to protect personal data would be assessed having regard to the volume and sensitivity of such personal data and the possible impact of a data breach. As stated in the Commission's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 17 May 2022) ("**Advisory Guidelines**") at paragraphs 17.3(a) and (b), an organisation should:

> *"a) design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;*
>
> *…*
>
> *c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of security*
>
> *…"*

11 In the present case, the Subject Data comprised a large volume of sensitive personal data affecting 141,412 individuals. Such data included names, NRIC numbers, bank account information and income statements. Given the nature of such

personal data, there was a heightened risk of identity theft and/or financial loss, which called for a higher standard of security arrangements.

12 For the reasons set out below the Commission determines that the Organisation failed to implement reasonable security arrangements to protect the Subject Data, in breach of the Protection Obligation. In particular, the Organisation failed to:

a) Conduct regular monitoring for software patches;

b) Implement processes to manage software patches and upgrades; and

c) Implement MFA for its administrator accounts.

Failure to conduct regular monitoring for software patches

13 The importance of conducting regular monitoring for software patches, and more generally testing the vulnerability of info-communications and technology ("**ICT**") systems, has been stressed repeatedly by the Commission.

14 In *Commeasure Pte Ltd* [2021] SGPDPC 11, the Commission highlighted at paragraph 14 that it was ***necessary*** for organisations to conduct regular reviews and monitoring of their ICT systems, which would include monitoring for software patches and updates.

15 The Commission has also made clear at page 27 of its *Guide to Data Protection Practices for ICT Systems*, that as a ***basic measure,*** organisations ought to "*conduct*

regular ICT monitoring, alerts, security audits, scan and tests to detect vulnerabilities and non-compliance with organisational standards."

16 However, the Organisation failed to conduct regular monitoring for software patches for the software on the Device. The Device (with the Vulnerability) had been in use by the Organisation since September 2019, more than 3 months since the Device's manufacturer had released the patch in May 2019. The Vulnerability remained un-patched for a period of almost 3 years thereafter until the Incident occurred. The Organisation admitted that it was unaware of the patch until after the Incident and that it did not conduct regular monitoring for software patches. Had the Organisation conducted regular monitoring for software patches, it would have learned of the patch for the Vulnerability.

17 Accordingly, the Commission finds the Organisation in breach of the Protection Obligation for its failure to conduct regular monitoring for software patches to the software on the Device.

Failure to implement processes to manage software patches and upgrades

18 The Organisation's failure to conduct regular monitoring for software patches underscores the importance for organisations to implement processes to manage the same.

19 As noted at paragraph 7(e) above, software patching was done on an ad-hoc basis by the Organisation's IT vendor on the instructions of the Organisation. However, as the Organisation failed to monitor for software patches, it was unaware of the

available patch for the Vulnerability, and did not instruct the IT vendor to install the patch.

20 Based on the Organisation's clarifications to the Commission, it is likely that the Organisation ***assumed*** that its IT vendor would monitor for software patches even though the Organisation's contract with its IT vendor did not contain any requirements for the IT vendor to conduct regular monitoring. The Organisation failed to properly apply its mind to the issue of regular monitoring, as this was not contained in the contract between the Organisation and its IT vendor.

21 In its *Checklists to Guard Against Common Types of Data Breaches*, the Commission recommends at page 6 that organisations should, as a ***basic practice***, "*Develop an ICT policy that covers the critical aspects in IT security such as account and access control, password, email, IT risk management, asset and configuration, backup and recovery, hardening and patching*."

22 While the Commission does not prescribe the specific terms of such ICT policies and/or processes, the Organisation could, for example, have implemented processes by which the Organisation or its IT vendors were automatically notified of available software patches, or reminded on a periodic basis to conduct checks for software patches. Further, the contract between the Organisation and its IT vendor could have specifically included an obligation for the IT vendor to conduct regular monitoring for patches, without the need for the Organisation to request patching on an ad-hoc basis. However, the Organisation failed to implement ***any*** such processes to manage software patches and upgrades.

23 For completeness, the Organisation provided the Commission with copies of its Internal Data Protection Policy and its Compliance Handbook. However, neither document sets out any processes to manage software patches and upgrades.

24 Accordingly, the Commission finds the Organisation in breach of the Protection Obligation for its failure to implement processes to manage software patches and upgrades.

Failure to implement MFA for administrator accounts

25 The Organisation also failed to implement MFA for its administrator accounts.

26 In its decision in *Lovebonito Singapore Pte. Ltd.* [2022] SGPDPC 3 published on 19 May 2022 (i.e. before the Incident), the Commission made clear that MFA was to be implemented as ***a baseline requirement*** for accounts with access to confidential or sensitive personal data or large volumes of personal data:

> "*Henceforth, the Commission adopts the following tiered approach:*
>
> *(a) First, 2FA / MFA should be implemented as a* ***baseline requirement for administrative accounts to systems that hold personal data of a confidential or sensitive nature, or large volumes of personal data****: see [46]-[47] above. Failure to do so can ipso facto amount to a breach, unless the organisation can show that its omission is reasonable or implementation of 2FA is disproportionate.*

(b) Second, ***remote access by privileged accounts to information systems that host confidential or sensitive personal data, or large volumes of personal data, should a fortiori be secured by 2FA / MFA****. The risks concerning remote access are higher, thus the expectation to implement 2FA / MFA will correspondingly increase.*

(c) Third, ***organisations using IT systems to host confidential or sensitive personal data, or large volumes of personal data, are expected to enable and configure 2FA / MFA****, if this is a feature that is available out-of-the-box. Omission to do so may be considered an aggravating factor*."[4] (emphasis added in bold)

27 However, the Organisation failed to implement MFA for its administrator accounts despite these accounts having access to confidential and sensitive personal data.[5] The Organisation did not furnish any explanation as to why such failure was reasonable or that the implementation of MFA would have been disproportionate.

28 Accordingly, the Commission finds the Organisation in breach of the Protection Obligation for its failure to implement MFA for its administrator accounts.

29 The Commission notes that the present case and the first tier of the approach in *Lovebonito Singapore Pte. Ltd*. [2022] SGPDPC 3 (reproduced at paragraph 25 above) deal specifically with administrator accounts. However, where an account is

[4] See *Lovebonito Singapore Pte. Ltd.* [2022] SGPDPC 3 at [51].
[5] "Sensitive" personal data includes, but is not limited to, NRIC/Passport numbers, financial information, and medical information. See the Commission's previous decisions in *Aviva Ltd* [2017] SGPDPC 14 at [17] and in *Genki Sushi Singapore Pte. Ltd*. [2019] SGPDPC 26 at [12] and [13].

not an administrator account, but is granted access rights to a database containing sensitive personal data records or a significant volume of personal data that would adversely impact the affected individuals in the event of a personal data breach, the Commission encourages organisations to consider implementing enhanced access controls to the account, such as through the use of a OTP or 2FA/MFA to better safeguard the personal data.

The Commission's Decision

30 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and if so, the amount of such financial penalty, the Commission took into account the factors listed at section 48J(6) of the PDPA.

31 The Commission notes that the data breach affected 141,412 individuals whose personal data, of a highly sensitive nature, was encrypted. Further, the patch for the Vulnerability had been available for a lengthy period of ***2 years and 9 months*** from the time the Organisation first started using the Device until the Incident, but was not installed during that time. The Organisation had also failed to implement MFA for its administrator accounts.

32 The Commission nevertheless recognises the following mitigating factors:

a) the Organisation was cooperative with the Commission's investigations;

b) the Organisation took prompt remedial actions to address the Incident; and

c) the Organisation had voluntarily accepted responsibility for the Incident, thus facilitating the expeditious investigation and resolution of this case through the expedited breach procedure.

33 Having considered all the relevant factors in this case, the Commission hereby requires the Organisation to pay a financial penalty of $82,000 within 30 days from the date of the relevant notice accompanying this decision, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

34 No further directions are necessary on account of the remedial measures already taken by the Organisation.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION